手 続 補 正 書

（法第１１条の規定による補正）

特許庁審査官　　石田　信行　殿

１．国際出願の表示　　ＰＣＴ／ＪＰ２００３／０１０１８６

２．出　願　人

名　称　　松下電器産業株式会社
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

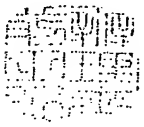
あて名　　〒５７１－８５０１　日本国大阪府門真市大字門真１００６番地
1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501 Japan

国　籍　　日本国　ＪＡＰＡＮ

住　所　　日本国　ＪＡＰＡＮ

３．代　理　人

氏　名　　弁理士（７７９３）前　田　　弘
MAEDA Hiroshi



あて名　　〒５４１－００５３
日本国大阪府大阪市中央区本町２丁目５番７号　大阪丸紅ビル
Osaka-Marubeni Bldg., 5-7, Hommachi 2-chome,
Chuo-ku, Osaka-shi, Osaka 541-0053 JAPAN

４．補正の対象

請求の範囲

5．補正の内容　　別紙添付書類に記載の通り。

（1）請求の範囲第２８頁第１項第８行目－第１０行目を、「入力された鍵データを用いたＥＣＢ（electronic code book）処理を行うことによって、ＣＢＣ（cipher block chaining）モード及びＣＦＢ（cipher feedback）モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで、前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを備え、」に補正し、第１項第１２行目－第１６行目を、請求の範囲第２９頁第４項第３行目－第２９行目の内容に補正する。

（2）請求の範囲第２９頁第４項を削除する。

（3）請求の範囲第３０頁－第３３頁の第５項－第１０項において、「請求項４」を「請求項１」に補正する。

（4）請求の範囲第３３頁第１１項第１行目を、請求の範囲第２８頁第１項第１行目－第７行目及び「入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで、前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックと、」に補正し、第１１項第７行目の「更に」を削除する。

（5）請求の範囲第３４頁第１３項第６行目，第７行目を、「入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができ

るように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで暗号化を行い、得られた暗号化結果を出力する共用処理ブロックとを備え、」に補正し、第１３項第９行目－第１１行目を、請求の範囲第３４頁第１４項第３行目－第２４行目の内容に補正する。

（６）請求の範囲第３４頁第１４項を削除する。

（７）請求の範囲第３５頁第１５項第６行目，第７行目を、「　入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで復号化を行い、得られた復号化結果を出力する共用処理ブロックとを備え、」に補正し、第１５項第９行目－第１１行目を、請求の範囲第３５頁第１６項第３行目－第２０行目の内容に補正する。

（８）請求の範囲第３５頁第１６項を削除する。

６．添付書類の目録

請求の範囲第２８頁、第２８／１頁、第２９頁－第３３頁、第３３／１頁、第３４頁、第３４／１頁、第３５頁、第３５／１頁、及び第３６頁　　各１通

請 求 の 範 囲

1．（補正後）　暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ（electronic code book）処理を行うことによって、ＣＢＣ（cipher block chaining）モード及びＣＦＢ（cipher feedback）モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで、前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第４のセレクタとを有するものであり、

前記ＥＣＢ処理器は、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

暗号化復号化装置。

２．　請求項１に記載の暗号化復号化装置において、

前記データ構造解析ブロックは、

前記暗号化データにおけるヘッダの解析を行い、前記ヘッダの情報に基づいて前記暗号化データからＭＡＣ（media access control）構造を抜き出し、前記ＭＡＣ構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該暗号化データが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記制御用データとして出力するとともに、前記ＭＡＣ構造デ

ータから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである

ことを特徴とする暗号化復号化装置。

３．　請求項１に記載の暗号化復号化装置において、

前記データ制御ブロックは、

前記制御用データに従って、前記処理ブロック入力データをＣＢＣモード、及びＣＦＢモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである

ことを特徴とする暗号化復号化装置。

４．（削除）

５．（補正後）　請求項１に記載の暗号化復号化装置において、

前記ビットマスク器は、

前記モード選択信号が５６ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものである

ことを特徴とする暗号化復号化装置。

６．（補正後）　請求項１に記載の暗号化復号化装置において、

前記第１のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前

記処理ブロック入力データを選択して出力し、その他の場合には、前記暗号処理データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

７．（補正後）　請求項１に記載の暗号化復号化装置において、

前記第２のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

８．（補正後）　請求項１に記載の暗号化復号化装置において、

前記第３のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であ

って、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

９．（補正後）　請求項１に記載の暗号化復号化装置において、

前記第４のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、前記暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものである

ことを特徴とする暗号化復号化装置。

１０．（補正後）　請求項１に記載の暗号化復号化装置において、

前記ＥＣＢ処理器は、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、暗号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＢＣモードであることを示す場合には、復号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がＣＦＢモードであることを示す場合には、暗号化処理を行うものである

ことを特徴とする暗号化復号化装置。

１１．（補正後）　暗号化データ又は暗号化すべきデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで、前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する共用処理ブロックと、

暗号化データ又は前記共用処理ブロックの出力を選択し、前記データ構造解析ブロックに出力する第１の入力セレクタと、

暗号化すべきデータ又は前記共用処理ブロックの出力を選択し、前記データ構

造解析ブロックに出力する第２の入力セレクタと、

所定の値又は前記共用処理ブロックの出力を選択し、出力する出力セレクタとを備え、

前記暗号化データ又は前記暗号化すべきデータに対して前記共用処理ブロックにおける処理が所定の回数行われると、前記出力セレクタが前記共用処理ブロックの出力を選択するように構成されている

ことを特徴とする暗号化復号化装置。

１２．　請求項１１に記載の暗号化復号化装置において、

前記所定の回数は、３回である

ことを特徴とする暗号化復号化装置。

１３．（補正後）　暗号化すべきデータを受け取り、そのデータ構造の解析を行って、制御用データを求めて出力するとともに、前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても暗号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで暗号化を行い、得られた暗号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第１のセレクタと、

前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第２のセレクタと、

前記第１のセレクタの出力と前記第２のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算

器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第４のセレクタとを有するものであり、

前記ＥＣＢ処理器は、

前記ＥＣＢ処理として暗号化処理を前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化装置。

１４．（削除）

１５．（補正後）　暗号化データを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

入力された鍵データを用いたＥＣＢ処理を行うことによって、ＣＢＣモード及びＣＦＢモードのいずれにおいても復号化を行うことができるように構成されており、前記処理ブロック入力データに対して、前記モード選択信号に示されたモードで復号化を行い、得られた復号化結果を出力する共用処理ブロックとを備え、

前記共用処理ブロックは、

前記ＥＣＢ処理を行い、得られた結果を暗号処理データとして出力するＥＣＢ処理器と、

前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタ

データ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第２のセレクタと、

前記暗号処理データと前記第２のセレクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択して出力する第３のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを有するものであり、

前記ＥＣＢ処理器は、

前記モード選択信号に従って、前記ＥＣＢ処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第３のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする復号化装置。

１６．（削除）

１７．　受信した信号をデータに変換して出力するダウンストリームＰＨＹ部と、

前記データからダウンストリームデータ及び鍵データを分離して出力するダウンストリームデータ処理部と、

前記鍵データを用いて前記ダウンストリームデータを復号化して出力する第１の暗号化復号化装置と、

M03-N-084CT1

答　弁　書

特許庁審査官　　石田　信行　殿

1．国際出願の表示　　ＰＣＴ／ＪＰ２００３／０１０１８６

2．出願人

名　称　　松下電器産業株式会社

MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

あて名　　〒５７１－８５０１　日本国大阪府門真市大字門真１００６番地

1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501 Japan

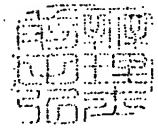
国　籍　　日本国　Ｊａｐａｎ

住　所　　日本国　Ｊａｐａｎ

3．代理人

氏　名　　弁理士　（７７９３）　前　田　　弘

MAEDA Hiroshi



あて名　　〒５４１－００５３

日本国大阪府大阪市中央区本町２丁目５番７号　大阪丸紅ビル

Osaka-Marubeni Bldg., 5-7, Hommachi 2-chome,

Chuo-ku, Osaka-shi, Osaka 541-0053 JAPAN

4．通知の日付　　２０．０４．２００４

５．答弁の内容

（１）見解の要点

本願に対し、２００４年４月２０日付けにて、下記の趣旨の見解の通知がありました。

文献１：ＪＰ，２０００－７５７８５，Ａ（富士通株式会社）

文献２：ＪＰ，７－２６１６６２，Ａ（富士通株式会社）

文献３：ＪＰ，１０－２１５２４４，Ａ（ソニー株式会社）

文献４：ＪＰ，２００１－１７７５１８，Ａ（日本電気株式会社）

請求の範囲１，２，１３，１５，１８－２０に係る発明は、文献１又は文献２と文献３及び文献４とにより、進歩性を有しない。つまり、文献１又は文献２の暗号化復号化装置に文献３及び文献４に記載された構成を用いて、ＣＢＣモード或いはＣＦＢモードを選択制御する構成とすることは、当業者にとって容易である。

請求の範囲３に係る発明は、文献１－４により、進歩性を有しない。

（２）答弁

上記の見解に対し、本願出願人は、今般、別途提出の手続補正書により、次のような補正を行いました。

すなわち、進歩性があるとの見解が示された請求の範囲４の限定事項を、請求の範囲１に加えました。同様に、請求の範囲１４の限定事項を請求の範囲１３に加え、請求の範囲１６の限定事項を請求の範囲１５に加えました。更に、請求の範囲４，１４，１６を削除し、請求の範囲１１を独立項になるように補正しました。

この補正により、請求の範囲１－１７に係る発明は、進歩性を有する発明になったものと考えます。

（３）結び

以上のように、本願請求の範囲のうち、請求の範囲１－１７に係る発明は、いずれも、文献１－４から容易に想到することができないものであるので、十分に進歩性を有するものと考えます。

以上、答弁申し上げます。